Information Warfare:
OPFOR Doctrine - An Integrated Approach

by MAJ Erin J. Gallogly-Staver, Threat Support Directorate
and MAJ Raymond S. Hilliard, Battle Command Training Program

This article was previously published in the *Military Intelligence Professional Bulletin* (MIPB).

The OPFOR information warfare (IW) doctrinal concept was approved by the Deputy Chief of Staff for Intelligence (DCSINT), Training and Doctrine Command (TRADOC), on 7 January 1997, and will be incorporated into the FM 100-60 series field manuals.[1] While the TRADOC Pamphlet 350-series discuss electronic combat, maskirovka, and camouflage, concealment, and deception, they reflect neither the realities of information-age technology nor recent writings by individuals associated with actual worldwide forces and organizations. Although the term "information warfare" is new to OPFOR doctrine, the concepts and principles that fall under the IW umbrella are not. The World Class OPFOR (WCOPFOR), Battle Command Training Program (BCTP), applies approximately 75 percent of the IW elements in all WARFIGHTERs. They continue to incorporate the doctrine and will implement IW, as a specific issue, during Corps and Division Seminars and WARFIGHTERs. Appropriately, the OPFOR considers IW to be evolutionary -- not revolutionary -- and as such, their application of it will continue to evolve. This article summarizes the approved doctrinal concepts, provides initial guidance to practitioners of OPFOR IW, and increases the awareness of U.S. Army commanders and trainers.

WHAT IS IW?

Many foreign forces and organizations have developed or are developing IW concepts, strategies, doctrine, and tactics, techniques, and procedures (TTP). Although there are many definitions, all contain an attack and defend dimension. The definition, shown below, provides a general framework for OPFOR IW strategies, campaigns, and operations.

Specifically planned and integrated actions taken to achieve an information advantage, at critical points and times. The OPFOR gains an advantage by affecting adversary information and information systems and defending OPFOR information and information systems.

The key components of this definition are integration and advantage. The OPFOR integrates its elements of power and targets specific enemy weaknesses while protecting its vulnerabilities. Not concerned about superiority or dominance, the OPFOR only seeks an advantage at critical points and times.

OPFOR IW does not equate to the U.S. concept of information operations (IO).[2] All elements of the OPFOR, to include sympathetic civilian populations, embrace IW as another means to compete. However, unlike the U.S., the OPFOR has no qualms or cultural aversion toward using deception, trickery, or civilian-run enterprises, such as hi-tech businesses or the media, when implementing an IW campaign. American citizens are by nature wary and skeptical of government involvement in IO. The OPFOR considers technology a double-edge sword and may occasionally use its unsophistication to its advantage; for instance, using commercially-available technology, such as cellular phones and messengers, instead of interlinked computers. The OPFOR can obtain high-tech equipment, such as frequency scanners, encryption devices, lasers, and digital video manipulation equipment, from the open or black markets. In most cases, it is more economical to purchase equipment or steal technology than develop systems independently. Finally, the OPFOR always seeks to exploit U.S. dependence on information-age technology and may attempt to overload U.S. intelligence collection efforts or disrupt a critical information link.

Figure 1 depicts the OPFOR IW doctrinal concept. The leadership of an OPFOR, whether from a terrorist group or the State, integrates all elements of power -- political, economic, military, and informational -- to implement its information strategy. One element of power may have primacy over the others during a certain operation or at a given time, but all are working together.

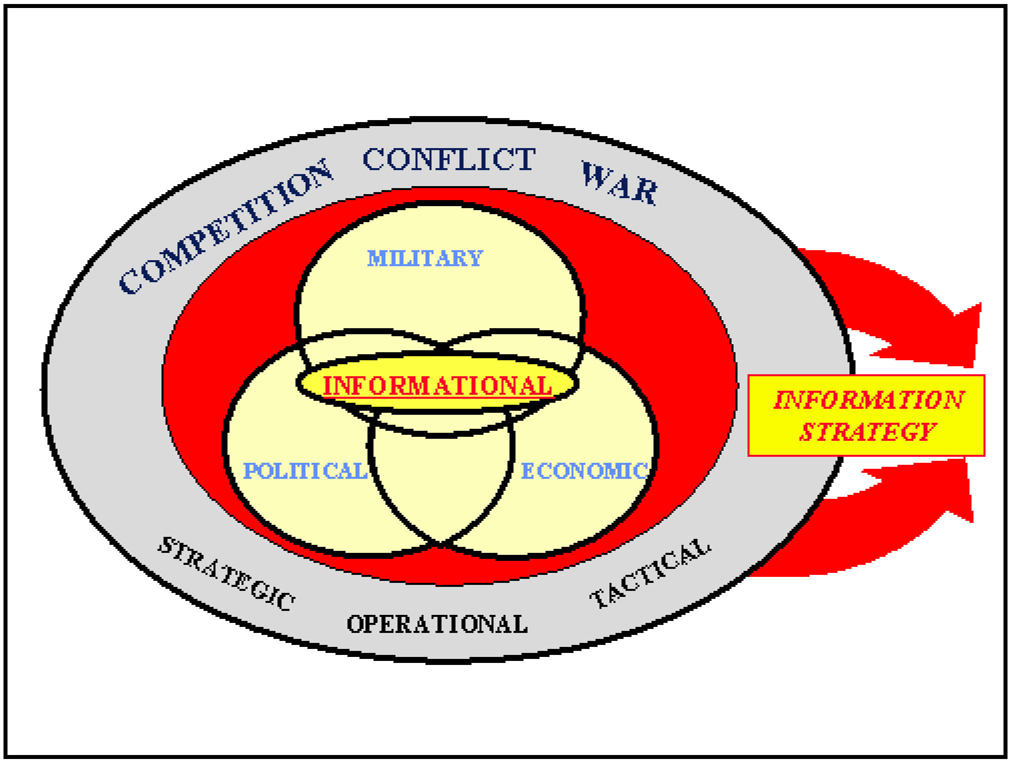
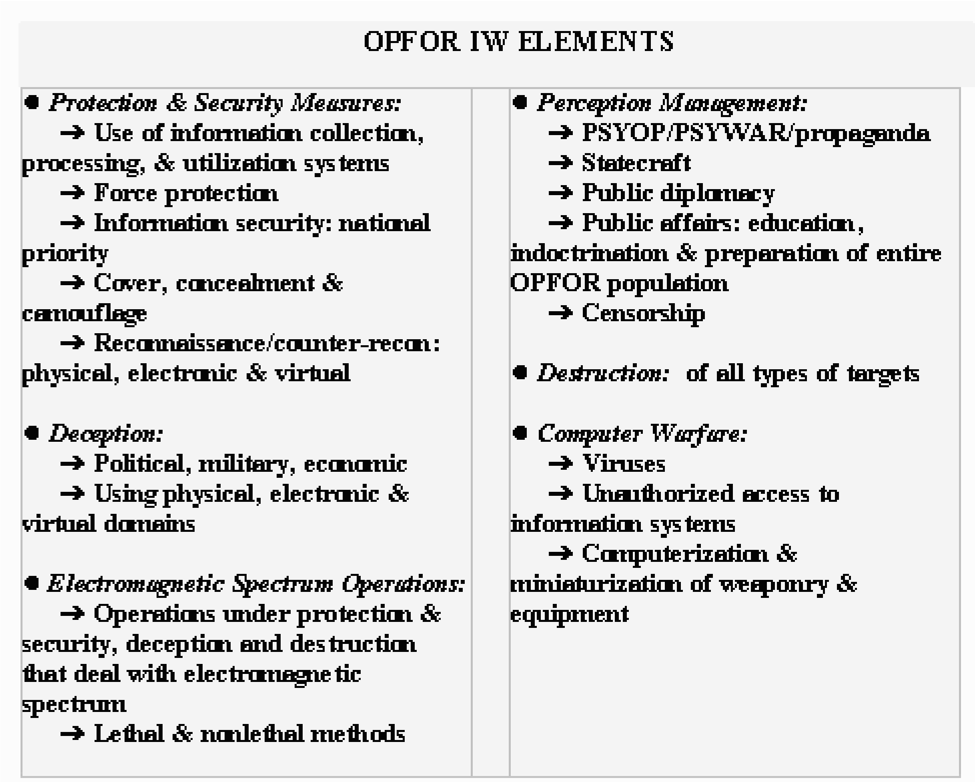


Figure 1. OPFOR Integration of IW

The outer ring of the diagram -- competition, conflict, and war -- illustrates the OPFOR concept that it is always trying to impose its will on someone; it is never at peace. The OPFOR conducts IW at all levels -- strategic, operational, and tactical -- and, in most instances, conducts an integrated IW campaign without regard to strict organizational boundaries. Research indicates that several foreign forces have a well-developed information strategy while others have one by default. For example, while Somali warlord Aideed probably did not have a formal integrated information strategy, one could conclude from his actions that he was using all his elements of power toward one goal -- getting the U.S. military out of Somalia.

OPFOR IW ELEMENTS

Across the operating continuum, the OPFOR considers six elements, described in Figure 2, when developing and implementing IW. Many subelements overlap. For example, if the OPFOR conducts electronic reconnaissance, it may be part of an electronic combat operation or part of protection and security measures, electromagnetic spectrum operations, and deception operations in an integrated IW campaign. Similarly, if the OPFOR disseminates a digitally-manipulated video that depicts its adversary conducting war crimes, that operation may be considered an integrated IW campaign comprising electromagnetic spectrum operations, perception management, deception, and computer warfare activities.



OPFOR IW ELEMENTS

● *Protection & Security Measures:* ➔ Use of information collection, processing, & utilization systems ➔ Force protection ➔ Information security: national priority ➔ Cover, concealment & camouflage ➔ Reconnaissance/counter-recon: physical, electronic & virtual ● *Deception:* ➔ Political, military, economic ➔ Using physical, electronic & virtual domains ● *Electromagnetic Spectrum Operations:* ➔ Operations under protection & security, deception and destruction that deal with electromagnetic spectrum ➔ Lethal & nonlethal methods		● *Perception Management:* ➔ PSYOP/PSYWAR/propaganda ➔ Statecraft ➔ Public diplomacy ➔ Public affairs: education, indoctrination & preparation of entire OPFOR population ➔ Censorship ● *Destruction:* of all types of targets ● *Computer Warfare:* ➔ Viruses ➔ Unauthorized access to information systems ➔ Computerization & miniaturization of weaponry & equipment

Figure 2. OPFOR IW Elements

Protection and security measures are broader than the U.S. concepts of operations security (OPSEC) and force protection. The OPFOR considers information a critical resource and takes appropriate protective measures such as censoring, camouflage, counter-reconnaissance, and encryption. It employs a variety of systems to collect, process, and use information to determine friendly and adversary weaknesses and vulnerabilities, assess various conduits for use in IW campaigns, and evaluate IW campaigns.

The OPFOR thoroughly integrates **deception** operations using all elements of power, within all domains -- physical, electronic, and virtual -- across the operating continuum. Economic organizations may publish false financial figures; official spokespersons may initiate a rumor campaign; the military may use decoys or conduct a feint, all integrated to mislead the adversary. Each deception operation has a specific target, objective, story, and means allocated to make it believable and, at least to some extent, verifiable. The OPFOR allocates sufficient resources to execute the deception operation so an adversary will believe the deception story. For example, a military commander may allocate up to 30 percent of his available combat power to create a combined-arms deception force in an effort to preserve combat power, achieve surprise, and gain an advantage on the battlefield.

Electromagnetic spectrum operations span the entire electromagnetic spectrum. These include, but are not limited to, operations that use radios, radar, lasers, directed-energy weapons, digital manipulation, parapsychology, holograms, morphing, and computers. The OPFOR applies both lethal and non-lethal methods, such as destroying a radio-relay site and blinding a soldier. Figure 3 illustrates examples of equipment used to conduct electromagnetic spectrum operations.

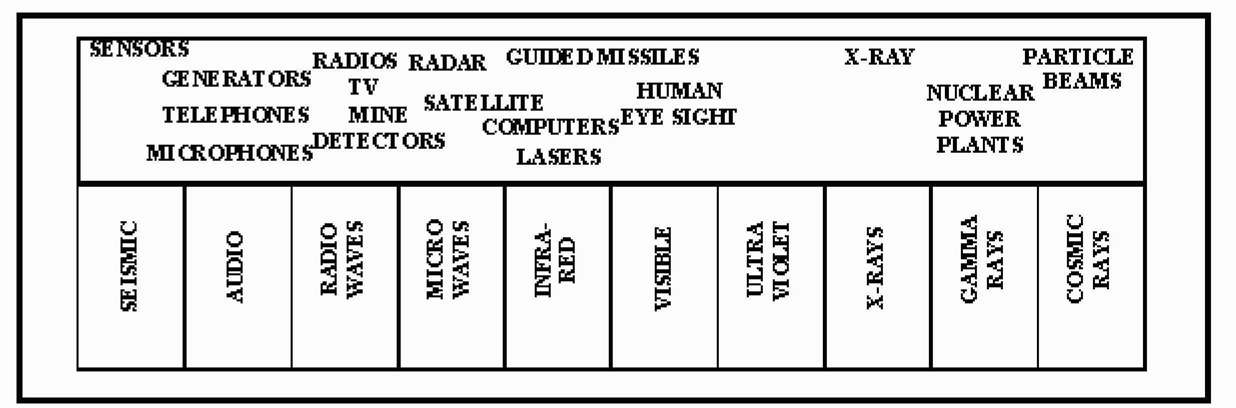


Figure 3. Electromagnetic Spectrum and Equipment

Perception management operations include all planned operations, against foreign and friendly targets, intended to change, manipulate, control, or otherwise manage a target's perceptions. Perception management is broader than U.S. psychological operations which target only foreign audiences. The OPFOR uses truth, false information, and misinformation and "spins" information to fit its needs -- sometimes highlighting certain aspects or carefully deleting harmful information. Censorship and public affairs programs, aimed at a population sympathetic to the OPFOR, are an important component of perception management. When conducting IW, the OPFOR skillfully uses the media and other neutral players, such as non-governmental organizations, to benefit its operations and deter adversary operations.

Destruction, when integrated with other elements of OPFOR IW, is powerful. The military element of power has primacy in this area. Military forces that conduct destruction operations are often unaware that they are involved in an integrated IW campaign. Forces, such as an artillery unit, direct-action cell, or special operations team, may receive a mission to destroy a target at a certain time or by using a particular technique. Upon completion, the force continues with other assigned missions. The destruction element of IW highlights the importance of precision-guided weapons or Asmartweapons. A technologically-advanced OPFOR will continue to research, develop, and employ weapons and equipment with sophisticated information components such as guided weapons, munitions, or global positioning systems. Its goal is to link real-time intelligence systems and long-range precision weapons within a faster decisionmaking cycle than its adversary. Less-sophisticated OPFOR, however, will continue to target high-value targets with available weapons systems such as artillery and attack helicopters.

Computer warfare is the newest and perhaps most ominous of all the OPFOR IW elements. Although it overlaps with other elements, computer warfare requires sophisticated expertise to conduct. The OPFOR may contract hackers, disgruntled employees, or other foreign agents to provide computer warfare assistance. By hiring these services, it reduces the possibility of tracing the act back to the OPFOR. Computer warfare includes altering data and performance characteristics through the use of viruses or other database manipulation techniques; unauthorized access, such as hacking; and computerization, miniaturization, and robotization of weaponry and equipment. The OPFOR exploits the availability of technology on the open and black markets to determine vulnerabilities in its adversary's information systems.

METHODS, MEANS, AND TARGETS

When the OPFOR develops an IW campaign, the leaders and planners utilize a number of methods (see Figure 4). For example, using disguised personnel or electronically mimicking an authorized user, the OPFOR may masquerade in an attempt to gain access to its adversary's information system. Similarly, the OPFOR may manipulate or deny service by destroying or degrading hardware and software used by its adversary. Since the OPFOR integrates operations, methods short of destruction may provide a bigger payoff than physically destroying a target.

OPFOR IW METHODS

- Detect: to discover or determine the existence of
- Deceive: to give a false impression; to mislead

Influence: to affect the actions of a person; sway

- Manipulate: to manage skillfully
- Disrupt: to interrrupt; total effect at a given time
- Degrade: to lower or impair; partial effect over time
- Deny: to negate; prohibit use of
- Destroy: to eliminate existence of

Figure 4. OPFOR IW Methods

The OPFOR understands the potentially global affects of its IW campaigns. Advances in information-age technology permit the OPFOR to use or target multiple players simultaneously. Figure 5 illustrates various means through which the OPFOR conducts IW and targets of IW.[3] As shown, there are literally endless means through which the OPFOR may conduct its IW campaign. Targets either make decisions or, by their position or access, can influence decisionmakers.

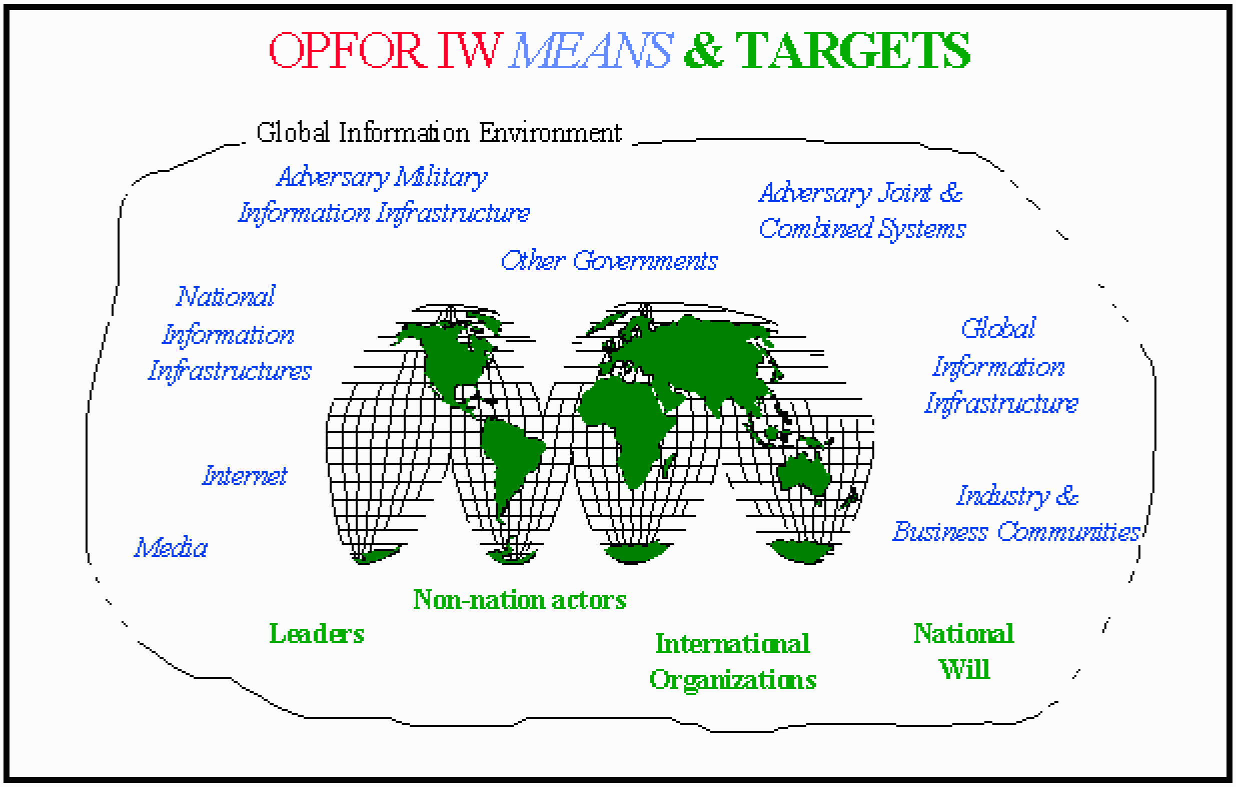

OPFOR IW MEANS & TARGETS
Global Information Environment
Adversary Military Information Infrastructure
Adversary Joint & Combined Systems
Other Governments
National Information Infrastructures
Global Information Infrastructure
Internet
Media
Industry & Business Communities
Non-nation actors
Leaders
International Organizations
National Will

Figure 5. OPFOR IW Means and Targets

Any person or organization with access to commercially available information technology and an information strategy can conduct IW. Commandante Marcos of the Zapatista rebels in Mexico and the Chinese students at Tianamen Square, for example, harnessed technology, had an information strategy, and marshaled international support for their causes. An OPFOR may have organizations with IW-type missions, such as a reconnaissance and electronic combat battalion, a direct-action cell of a terrorist group, a front company of a drug organization, or an artillery brigade. Some of these organizations require specialized equipment, such as jammers, to conduct electronic suppression or precision-guided weapons to conduct strikes against high-value targets. When considering the capabilities of an OPFOR to conduct IW, the trainer should consider various organic and commercially available equipment and organizations that have the potential to conduct IW-type missions. Lack of traditional military-type equipment, such as jammers and artillery, does not imply that an OPFOR cannot conduct an integrated IW campaign. The limiting factor in implementing IW is not technology, but rather the imagination and resolve of OPFOR leaders.

HISTORICAL EXAMPLE

The example below demonstrates the potential power of integrated IW. The Allies had an information strategy, developed a campaign, and executed various operations in support of the campaign. Trainers could use this historical example as a model, but employ modern weaponry and equipment and information-age technology.

THE NORMANDY INVASION
(June 1944)

When the Allied leadership decided to conduct an amphibious landing in Europe, they knew they had to improve on previous landings in North Africa and Italy. They decided to conduct a deception operation; planners developed numerous deception plans and supporting operations. The Allies employed many methods, to include psychological warfare (PSYWAR), political warfare, operations security (OPSEC), counterintelligence, electronic warfare, and human intelligence, in support of the operation. They used a variety of techniques, such as decoys, false units and radio traffic, PSYWAR broadcasts and leaflets, and chaff, in addition to adhering to strict OPSEC procedures. The results were positive -- Hitler did not reinforce troops in Normandy or Cherbourg.

DECEPTION GOAL: Allies protect the place, time, and extent of the Allied landing in Europe from the intelligence systems serving Hitler and the German High Command until D+30.

DECEPTION OBJECTIVE: Cause German leadership to scatter military reinforcements throughout Europe so they cannot reinforce Normandy or Cherbourg.

MEANS EMPLOYED: False units established, diplomatic negotiations, disguised actors, planted documents, human & counter-intelligence, decoys & dummies, tactical & logistical actions, broadcasts, leaflets.

CONDUITS: Double agents, signals intelligence, Luftwaffe, radar sites along coast, soldiers, senior German officers.

The FM 100-60 series field manuals will incorporate this new evolving OPFOR IW doctrine. As part of the capabilities-based OPFOR doctrine, the combat training centers, U.S. Army centers and schools, and future simulations will adapt and implement this doctrine in training. Fundamental to this OPFOR IW doctrinal concept is the integration of diverse capabilities at all levels, across the operating continuum, toward achieving an information strategy.

NOTE: MAJ Erin J. Gallogly-Staver is a student at the CGSOC. E-mail address is gallogle@leav-emh1.army.mil

---

[1] See MIPB, Oct-Dec 96, pp. 51-52, for more information on the OPFOR field manuals and pamphlets and the capabilities-based OPFOR.

[2] See. FM 100-6, *Information Operations*, August 1996, and Joint Pub 3-13, 1st Draft, *Joint Doctrine for Information Operations*, 21 January 1997, for additional information.

[3] The words in *italics* indicate means through which the OPFOR conducts IW. The words in **bold** indicate targets of IW and means through which the OPFOR conducts IW.